FEDERAL CRITERIA

LEGAL AUTHORITIES

- National Security Act of 1947
- Privacy Act of 1974
- Federal Managers' Financial Integrity Act of 1982
- Computer Fraud and Abuse Act of 1986
- Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended
- Computer Security Act of 1987
- Paperwork Reduction Act of 1995
- Clinger-Cohen Act of 1996 or Federal Acquisition Reform Act of 1996
- Computer Security Enhancement Act of 1997
- Government Information Security Reform

PRESIDENTIAL POLICIES

- PDD-62, *Combating Terrorism: Presidential Decision Directive 62*, May 22, 1998
- PDD-63, White Paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* May 22, 1998
- PDD-NCS-67, *Enduring Constitutional Government and Continuity of Government Operations*, 21 October 1998
- Executive Order, *Providing for the Physical Security of Facilities Important to the National Defense*, EO 10421, December 31, 1952
- Executive Order, *Assignment of national security and emergency preparedness telecommunications functions*, EO 12472, April 3, 1984
- Executive Order, *Assignment of Emergency Preparedness Responsibilities*, EO 12656, November 18,1998
- Executive Order, *Classified National Security Information*, EO 12958, April 17, 1995
- Executive Order, *National Infrastructure Assurance Council*, EO 13130, July 14, 1999
- OMB Circular No. A-123 revised, *Management Accountability and Control*, June 21, 1995
- OMB Circular No. A-127--revised, *Financial Management Systems*, July 23, 1993
- OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, November 28, 2000
- Critical Infrastructure Assurance Office, *Vulnerability Assessment Framework 1.1*, October 1998
- Critical Infrastructure Assurance Office, *National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*, January 2000.

INFORMATION SECURITY DIRECTIVES

- National Computer Security Center, *National Policy for Safeguarding and Control of Communications Security Material*, NCSC No. 1, 16 January 1981
- National Computer Security Center, *National Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments*, NCSC No. 5, 16 January 1981

- National Computer Security Center, *National Policy on Secure Voice Communications*, NCSC No. 8, 7 May 1982
- National Telecommunications and Information System Security Policy, *National Policy for Granting Access to U.S. Classified Cryptographic Information*, NTISS No. 3, 19 December 1988
- National Telecommunications and Information System Security Policy, *National Policy on Controlled Access Protection*, NTISS No. 200, 15 July 1987
- National Security Telecommunications and Information System Security Policy, *National Policy on Control of Compromising Emanations*, NSTISSP No. 300, 29 November 1993
- National Security Telecommunications and Information System Security Directive, *Information Systems Security (INFOSEC) Education, Training, and Awareness*, NSTISSD No. 500, 25 February 1993
- National Security Telecommunications and Information Systems Security Directive, *National Security Telecommunications and Automated Information Systems Security*, NSTISSD No. 502, 5 February 1993
- National Telecommunications and Information System Security Directive, *Communications Security (COMSEC) Monitoring*, NTISS No. 600, 10 April 1990
- National Security Telecommunications and Information Systems Security Directive, *Governing Procedures of the National Security Telecommunications and Information Systems Security Committee (NSTISSC)*, NSTISSD No. 900, April 2000
- Director of Central Intelligence Directive 1/16, *Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks*, 19 July 1988

OTHER GOVERNMENTWIDE POLICIES

- National Institute of Standards and Technology, Special Publication, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, NIST SP No. 800-16, April 1998
- National Institute of Standards and Technology, Special Publication, *Guide for Developing Security Plans for Information Technology Systems*, NIST SP No. 800-18, December 1998
- National Security Telecommunications and Information Systems Security Instructions, *Communications Security Equipment Maintenance & Maintenance Training*, NSTISSI No. 4000, January 1998
- Federal Preparedness Circular, *Continuity of the Executive Branch of the Federal Government at the Headquarters Level During National Security Emergencies*, FPC No. 60, November 20, 1990
- Federal Preparedness Circular, *Federal Executive Branch Continuity of Operations (COOP)*, FPC No. 65, July 26, 1999
- 5 CFR Part 930, *Programs for Specific Positions and Examinations (Miscellaneous)*, January 1, 2000

APPENDIX B

LIST OF RELEVANT OFFICE OF INSPECTOR GENERAL AND GENERAL ACCOUNTING OFFICE DOCUMENTS

Department of State Office of Inspector General

- *Computer Security Reviews of Paris Accounting & Disbursement System and Consolidated American Payroll Processing System*, Report No. 00-FM-014, June 2000.
- *Followup Audit of Domestic Telephone Security*, Report No. OSO/A-95-25, July 1995.
- *Audit of the Management of Secure Communications*, Report No. SIO/A-97-15, March 1997
- *Audit of Overseas Telephone Systems Security Management*, Report No. SIO/A-00-01, November 1999.
- *Security Inspection of State Annex 26, Beltsville, Maryland*, Report No. SIO/I-00-40, July 2000.

General Accounting Office

- *Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations*, GAO/AIMD-98-145, Washington, D. C., May 1998.
- *Executive Guide, Information Security Management, Learning from Leading Organizations*. Washington, D.C., May 1998
- *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, Washington D. C., January 1999
- *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110, Washington, D.C., September 24, 1996.

GOVERNMENTWIDE INFORMATION SECURITY AWARENESS AND TRAINING REQUIREMENTS

The Computer Security Act of 1987 requires mandatory periodic security awareness and training in accepted security practices for everyone involved in managing, using, or operating sensitive cyber systems. The training is required to enhance awareness of cyber vulnerabilities and threats, and encourage improved security practices. The procedures, scope, and manner of the security awareness and training must comply with NIST and OPM guidance.

Under 5 CFR Part 930, Subpart C, Employees Responsible for the Management or Use of Federal Computer Systems, OPM requires information technology security training for new employees within 60 days of hiring. OPM requires that all employees receive the training when they enter new positions dealing with sensitive information, or when their information security environment or procedures change significantly. The OPM guidance references the more extensive and detailed NIST guidance. OPM also requires periodic refresher training.

NIST Special Publication 800-16 is based on the Information Technology Security Body of Knowledge, Topics, and Concepts. The guidance describes beginning, intermediate, and advanced training agencies should give to executives, program and functional managers, IRM security and audit staff, automated data processing management and operations, and end users. The training should focus on computer security basics, planning and management, policies and procedures, contingency planning, and life cycle management.

The results-based guidance provides an integrated framework for identifying training needs throughout the organization and ensuring that everyone receives appropriate training. In emphasizing roles and responsibilities, the guidance provides instructions on measuring individual effectiveness in implementing information technology security policies and organizational effectiveness in providing the necessary awareness and training for those occupying all relevant positions.

The National Policy for the Security of National Security Telecommunications and Information Systems assigned NSTISSC[21] responsibility for developing and implementing a comprehensive approach to protecting national security information systems. The Committee sees education, training, and awareness as countermeasures that can effectively reduce U.S. Government exposure to known risks, but only if all employees are aware of and educated about information security problems involving telecommunications and information systems.

NSTISSC has issued National Telecommunications and Information Systems Security Directives (NTISSD) and National Security Telecommunications and Information Systems

[21] National Security Telecommunications and Information Systems Security Committee was created by National Security Directive No. 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated July 5, 1990. National Security Telecommunications and Information Systems Security Committee is authorized to issue operating policies to assure the security of telecommunications and automated information systems that process and communicate classified national security information and other sensitive information.

Security Instructions (NSTISSI) providing standards for information assurance education, training, and awareness.

- NSTISSD No. 500 – Information Systems Security (INFOSEC) Education, Training, and Awareness
- NSTISSD No. 501 – National Training Program for Information Systems Security (INFOSEC) Professionals
- NSTISSI No. 4011 – National Training Standard for INFOSEC Professionals
- NSTISSI No. 4012 – National Training Standard for Designated Approving Authority
- NSTISSI No. 4013 – National Training Standard for System Administrators in Information Systems Security (INFOSEC)
- NSTISSI No. 4014 – National Training Standard for Information Systems Security Officers (ISSO)

U.S. Strategy for International Outreach on Critical Infrastructure Protection[22]

Key Points:

A sound long-term strategy to protect U.S. critical infrastructures depends on not only implementation of our national plan, but on appropriately communicating our plan and cooperating with other states and international organizations. The exponential geographic spread of Information Technology, the rapidly evolving nature of information technology itself, the difficulty in predicting future threats and trends, and the need to effectively target limited U.S. resources all commend a strategy that is broad-based and flexible.

The U.S. Government already conducts a wide range of bilateral and multilateral CIP-related initiatives, in the context of international standards discussions, law enforcement, national security, and research and development. Private enterprises and industry groups also interact with foreign counterparts regularly. Such ad hoc efforts, however, can be less effective and slow to develop without high-level, government-to-government contacts to encourage CIP cooperation as a national priority. Uncoordinated agency efforts also can lead to foreign governments receiving mixed or incorrect messages about U.S. national CIP policy.

The U.S. international strategy aims to coordinate CIP outreach to other governments and international intergovernmental organizations by promoting CIP awareness, emphasizing vigilance in security standards and practices, and enhancing law enforcement cooperation as basic elements of the strategy for addressing CIP threats. Building on this foundation, the U.S. will pursue initiatives to address economic security and national security issues.

The U.S., through an interagency working group under State Department leadership, will establish agendas for government-to-government work on CIP and coordinate U.S. involvement in international intergovernmental organizations. The priorities will reflect the extent to which U.S. infrastructure is interdependent with that of any particular country or group of countries. The measure will be the number of economic sectors (telecommunications, energy, etc.) and government functions (defense, law enforcement, etc.) in other countries where there are significant interdependencies and opportunities for cooperative effort.

- For those countries where the U.S. has multiple interests or dependencies, the State Department will manage extensive interagency cooperation with the foreign government and will, together with CIP Sector Coordinators and liaisons, track the various U.S. interests to ensure consistency.

- For countries where the U.S. has more limited interests or dependencies, the scope of diplomatic contact and interagency coordination will be more limited. Bilateral

[22] Source: Assistant Secretary for International Narcotics and Law Enforcement Affairs.

government consultations will raise CIP awareness, address law enforcement issues, and focus on key U.S. national security and economic sector concerns. CIP Sector Coordinators will keep State informed of their activities.

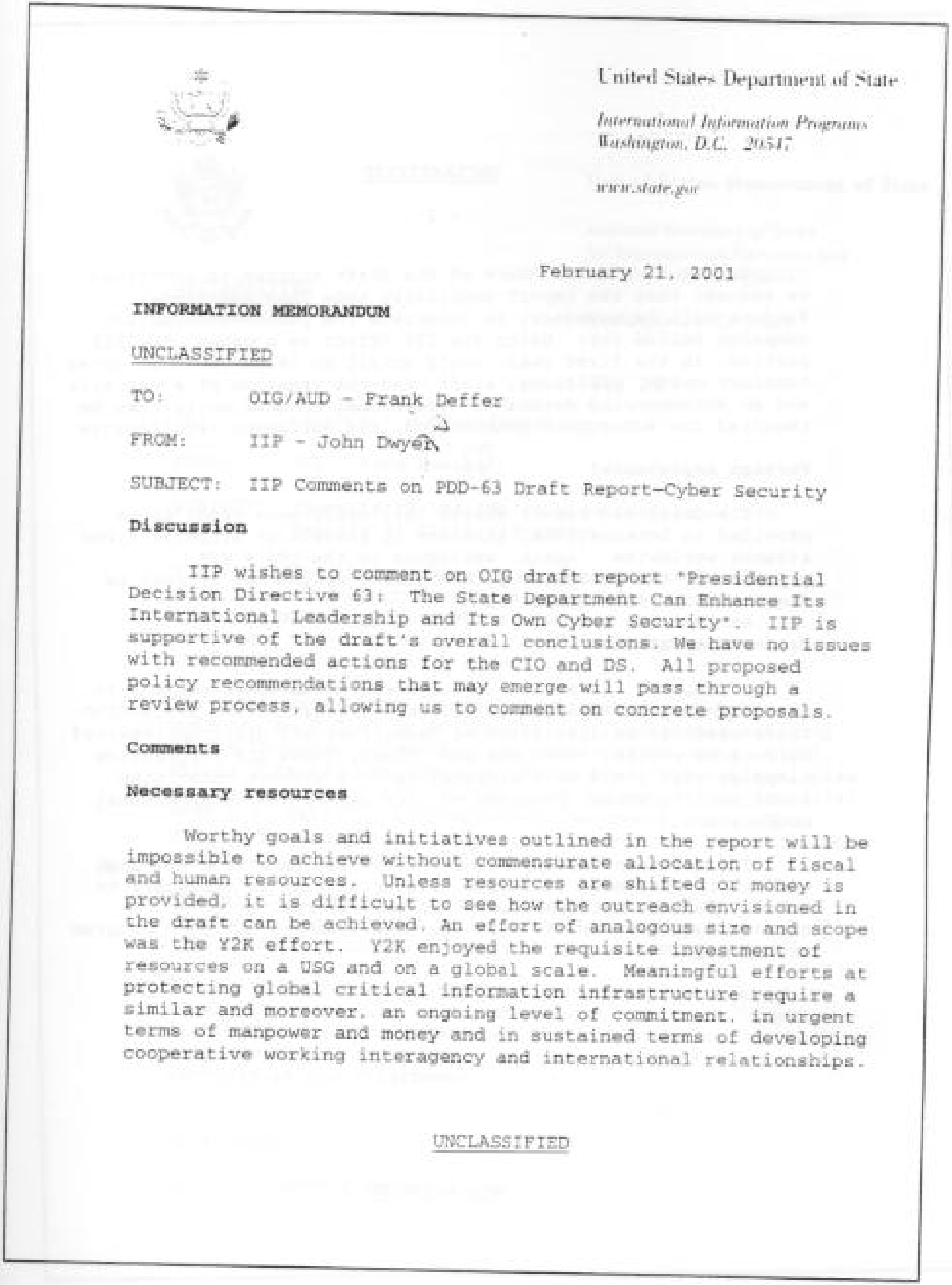
- For selected countries where the U.S. does not presently have direct dependency, the U.S. Government will, within the bounds of its resources, work to raise CIP awareness and to address legal frameworks and law enforcement issues.

- For international intergovernmental organizations, the State Department will coordinate activities, ensure common approaches across organizations, and prevent unnecessary duplication.

- Research and development in the Information Technology field is a largely international enterprise. Since most of this R&D has been developed in the unclassified commercial and academia sectors, it serves the U.S. national interest to draw on this global science and technology base. The U.S. Government will also continue to support, where appropriate, research that promotes national interests.

In all cases, the U.S. Government role will be limited and will seek to include industry input where appropriate. U.S. Government components will work with their counterparts in other countries to identify and address national security dependencies, and to facilitate private-sector cooperation, to raise awareness of potential problems, and to stimulate private - sector solutions. The U.S. Government will ensure proper protection of national security information and any sensitive data provided by foreign partners.

APPENDIX E



United States Department of State

International Information Programs
Washington, D.C. 20547

www.state.gov

February 21, 2001

INFORMATION MEMORANDUM

UNCLASSIFIED

TO: OIG/AUD - Frank Deffer

FROM: IIP - John Dwyer

SUBJECT: IIP Comments on PDD-63 Draft Report—Cyber Security

Discussion

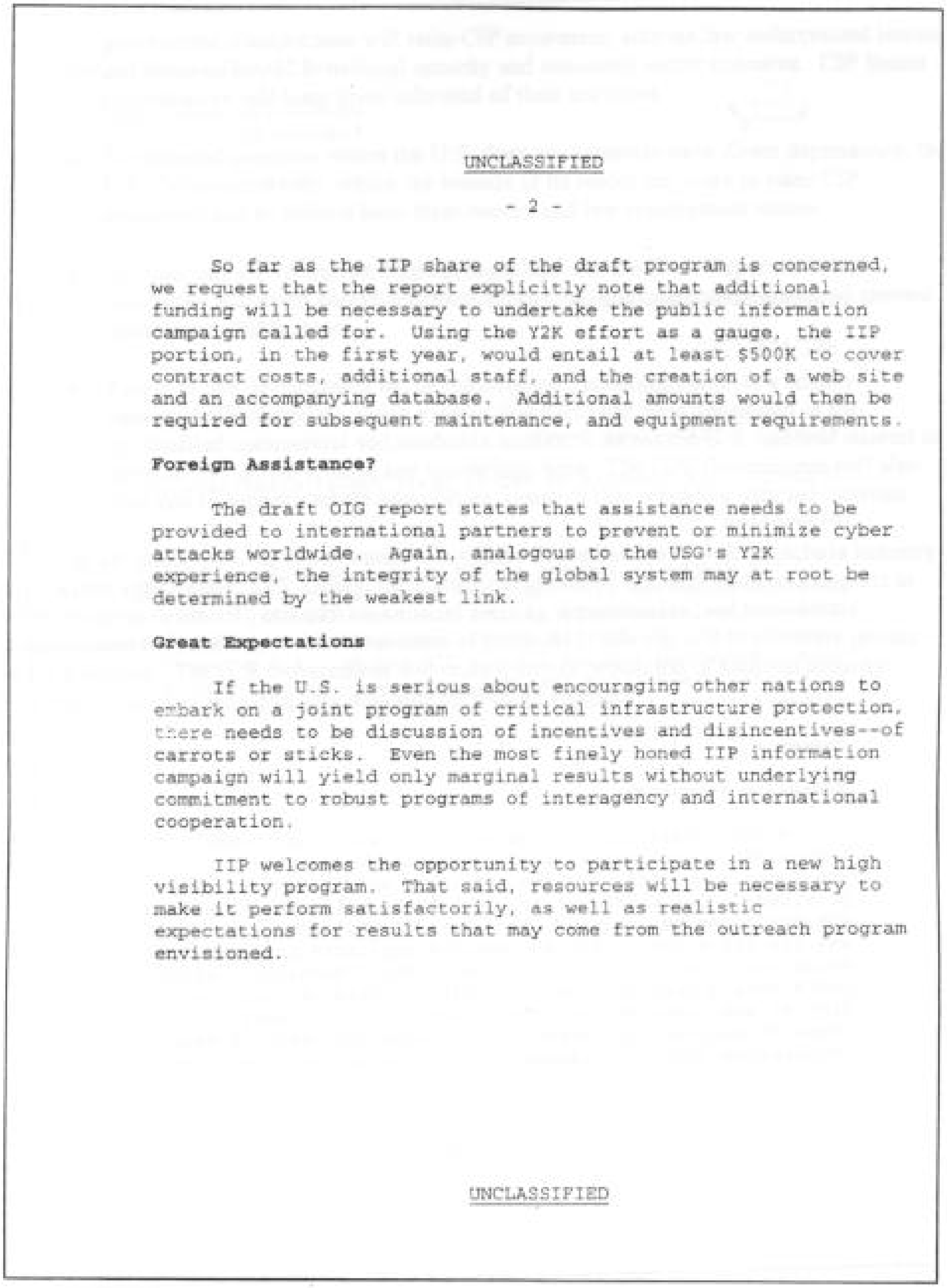
IIP wishes to comment on OIG draft report "Presidential Decision Directive 63: The State Department Can Enhance Its International Leadership and Its Own Cyber Security". IIP is supportive of the draft's overall conclusions. We have no issues with recommended actions for the CIO and DS. All proposed policy recommendations that may emerge will pass through a review process, allowing us to comment on concrete proposals.

Comments

Necessary resources

Worthy goals and initiatives outlined in the report will be impossible to achieve without commensurate allocation of fiscal and human resources. Unless resources are shifted or money is provided, it is difficult to see how the outreach envisioned in the draft can be achieved. An effort of analogous size and scope was the Y2K effort. Y2K enjoyed the requisite investment of resources on a USG and on a global scale. Meaningful efforts at protecting global critical information infrastructure require a similar and moreover, an ongoing level of commitment, in urgent terms of manpower and money and in sustained terms of developing cooperative working interagency and international relationships.

UNCLASSIFIED



So far as the IIP share of the draft program is concerned, we request that the report explicitly note that additional funding will be necessary to undertake the public information campaign called for. Using the Y2K effort as a gauge, the IIP portion, in the first year, would entail at least $500K to cover contract costs, additional staff, and the creation of a web site and an accompanying database. Additional amounts would then be required for subsequent maintenance, and equipment requirements.

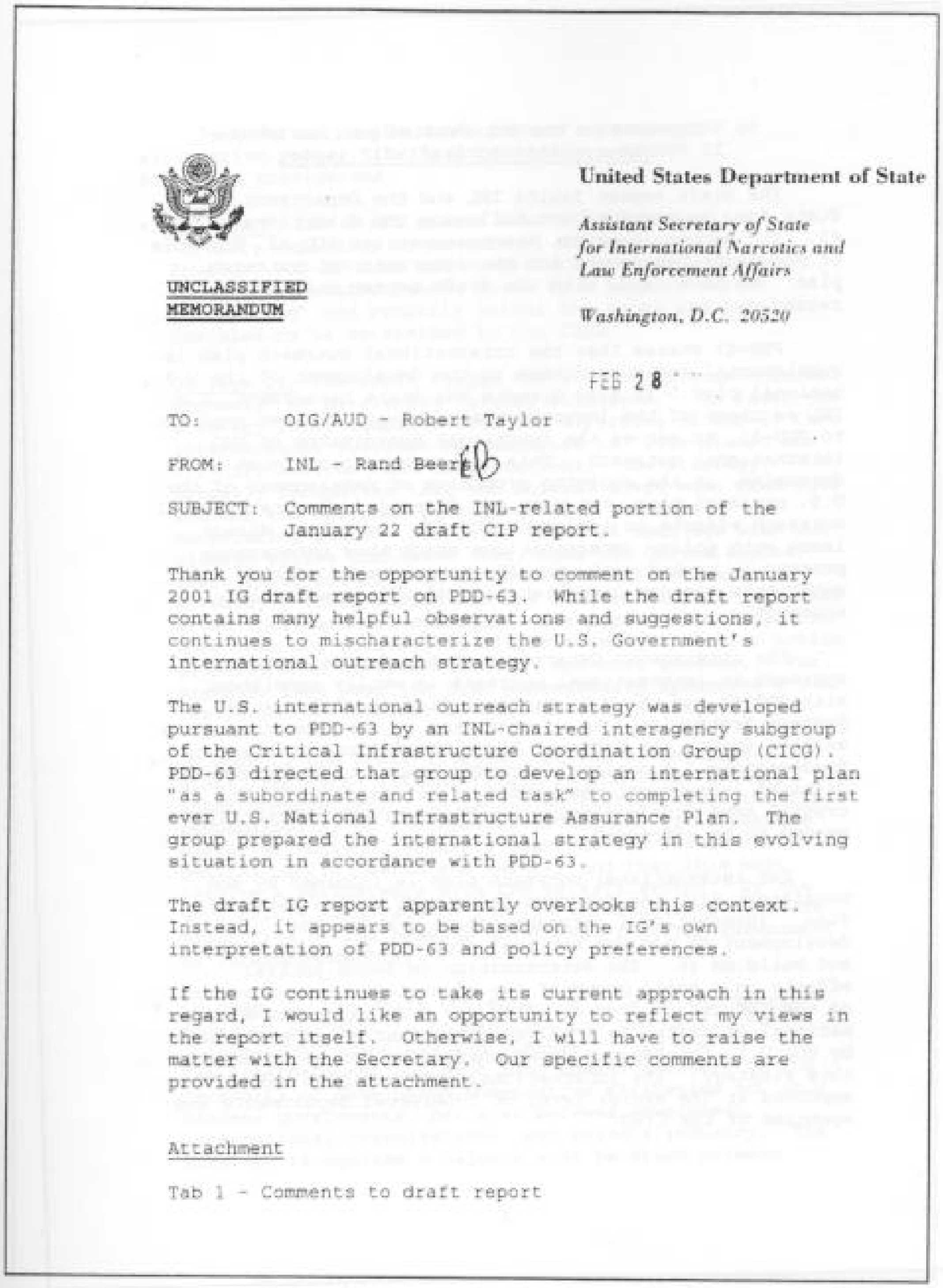
Foreign Assistance?

The draft OIG report states that assistance needs to be provided to international partners to prevent or minimize cyber attacks worldwide. Again, analogous to the USG's Y2K experience, the integrity of the global system may at root be determined by the weakest link.

Great Expectations

If the U.S. is serious about encouraging other nations to embark on a joint program of critical infrastructure protection, there needs to be discussion of incentives and disincentives--of carrots or sticks. Even the most finely honed IIP information campaign will yield only marginal results without underlying commitment to robust programs of interagency and international cooperation.

IIP welcomes the opportunity to participate in a new high visibility program. That said, resources will be necessary to make it perform satisfactorily, as well as realistic expectations for results that may come from the outreach program envisioned.



United States Department of State

Assistant Secretary of State
for International Narcotics and
Law Enforcement Affairs

Washington, D.C. 20520

UNCLASSIFIED
MEMORANDUM

FEB 28

TO: OIG/AUD - Robert Taylor

FROM: INL - Rand Beers

SUBJECT: Comments on the INL-related portion of the January 22 draft CIP report.

Thank you for the opportunity to comment on the January 2001 IG draft report on PDD-63. While the draft report contains many helpful observations and suggestions, it continues to mischaracterize the U.S. Government's international outreach strategy.

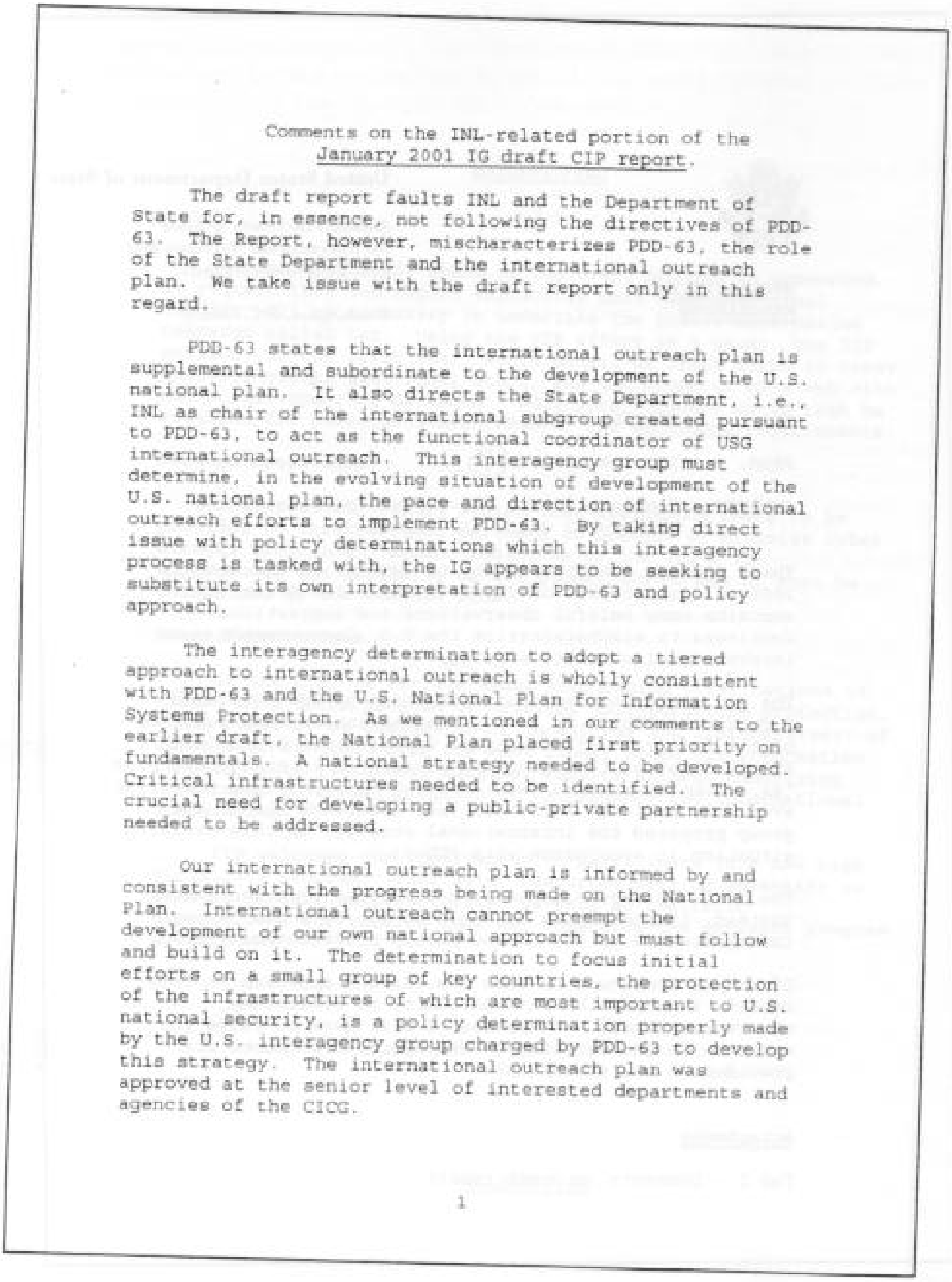
The U.S. international outreach strategy was developed pursuant to PDD-63 by an INL-chaired interagency subgroup of the Critical Infrastructure Coordination Group (CICG). PDD-63 directed that group to develop an international plan "as a subordinate and related task" to completing the first ever U.S. National Infrastructure Assurance Plan. The group prepared the international strategy in this evolving situation in accordance with PDD-63.

The draft IG report apparently overlooks this context. Instead, it appears to be based on the IG's own interpretation of PDD-63 and policy preferences.

If the IG continues to take its current approach in this regard, I would like an opportunity to reflect my views in the report itself. Otherwise, I will have to raise the matter with the Secretary. Our specific comments are provided in the attachment.

Attachment

Tab 1 - Comments to draft report



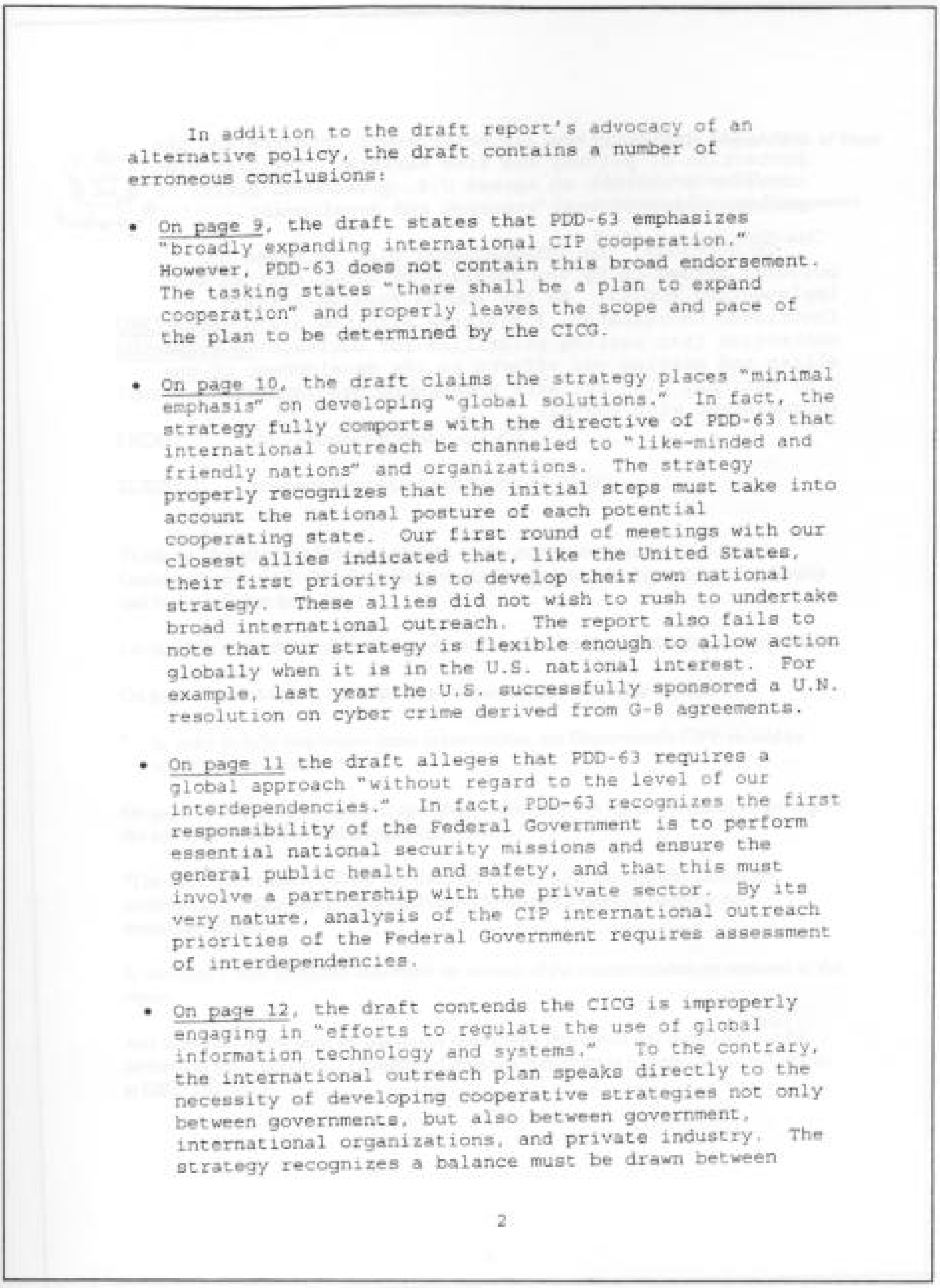
Comments on the INL-related portion of the January 2001 IG draft CIP report.

The draft report faults INL and the Department of State for, in essence, not following the directives of PDD-63. The Report, however, mischaracterizes PDD-63, the role of the State Department and the international outreach plan. We take issue with the draft report only in this regard.

PDD-63 states that the international outreach plan is supplemental and subordinate to the development of the U.S. national plan. It also directs the State Department, i.e., INL as chair of the international subgroup created pursuant to PDD-63, to act as the functional coordinator of USG international outreach. This interagency group must determine, in the evolving situation of development of the U.S. national plan, the pace and direction of international outreach efforts to implement PDD-63. By taking direct issue with policy determinations which this interagency process is tasked with, the IG appears to be seeking to substitute its own interpretation of PDD-63 and policy approach.

The interagency determination to adopt a tiered approach to international outreach is wholly consistent with PDD-63 and the U.S. National Plan for Information Systems Protection. As we mentioned in our comments to the earlier draft, the National Plan placed first priority on fundamentals. A national strategy needed to be developed. Critical infrastructures needed to be identified. The crucial need for developing a public-private partnership needed to be addressed.

Our international outreach plan is informed by and consistent with the progress being made on the National Plan. International outreach cannot preempt the development of our own national approach but must follow and build on it. The determination to focus initial efforts on a small group of key countries, the protection of the infrastructures of which are most important to U.S. national security, is a policy determination properly made by the U.S. interagency group charged by PDD-63 to develop this strategy. The international outreach plan was approved at the senior level of interested departments and agencies of the CICG.



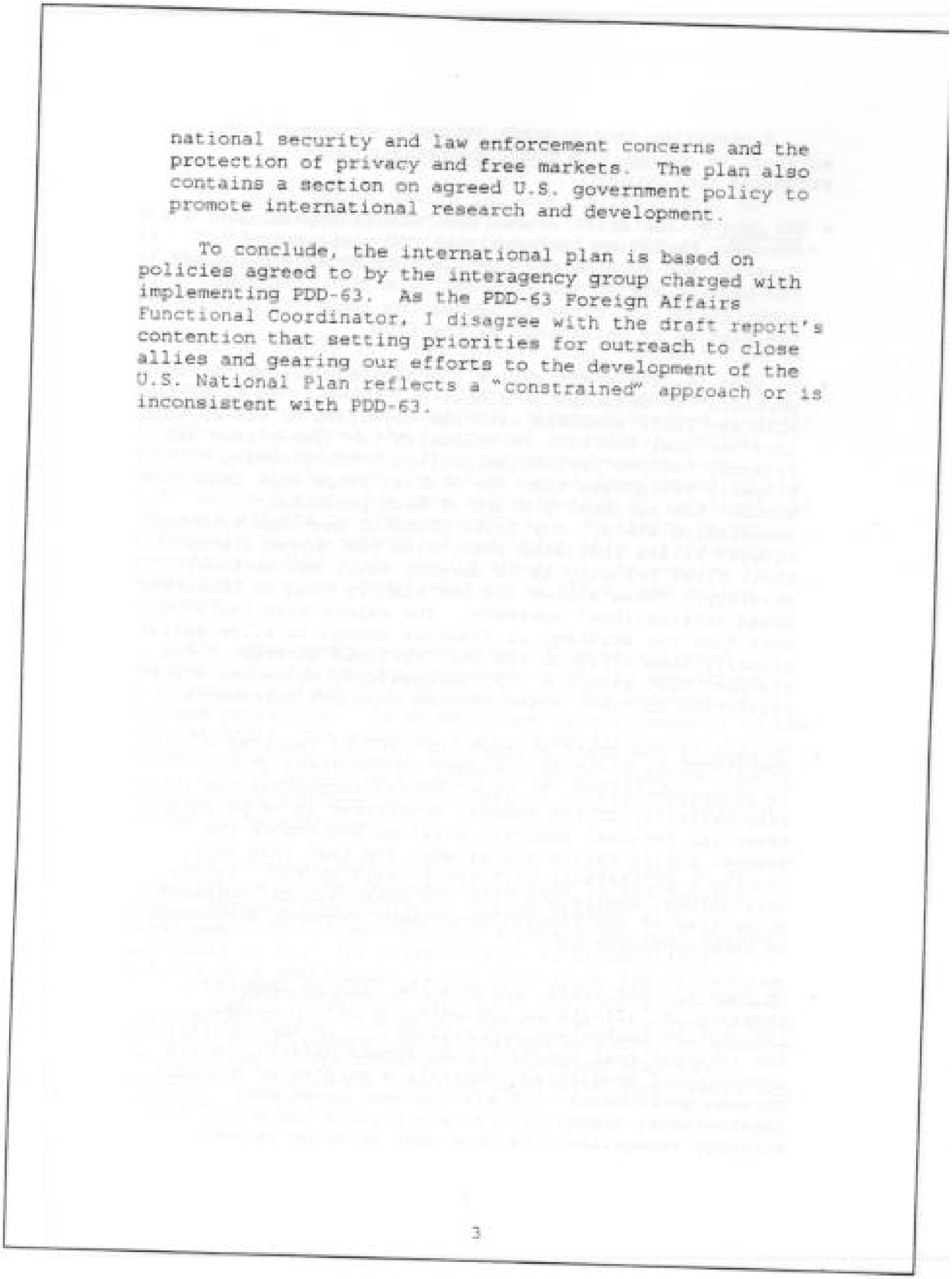
In addition to the draft report's advocacy of an alternative policy, the draft contains a number of erroneous conclusions:

- On page 9, the draft states that PDD-63 emphasizes "broadly expanding international CIP cooperation." However, PDD-63 does not contain this broad endorsement. The tasking states "there shall be a plan to expand cooperation" and properly leaves the scope and pace of the plan to be determined by the CICG.

- On page 10, the draft claims the strategy places "minimal emphasis" on developing "global solutions." In fact, the strategy fully comports with the directive of PDD-63 that international outreach be channeled to "like-minded and friendly nations" and organizations. The strategy properly recognizes that the initial steps must take into account the national posture of each potential cooperating state. Our first round of meetings with our closest allies indicated that, like the United States, their first priority is to develop their own national strategy. These allies did not wish to rush to undertake broad international outreach. The report also fails to note that our strategy is flexible enough to allow action globally when it is in the U.S. national interest. For example, last year the U.S. successfully sponsored a U.N. resolution on cyber crime derived from G-8 agreements.

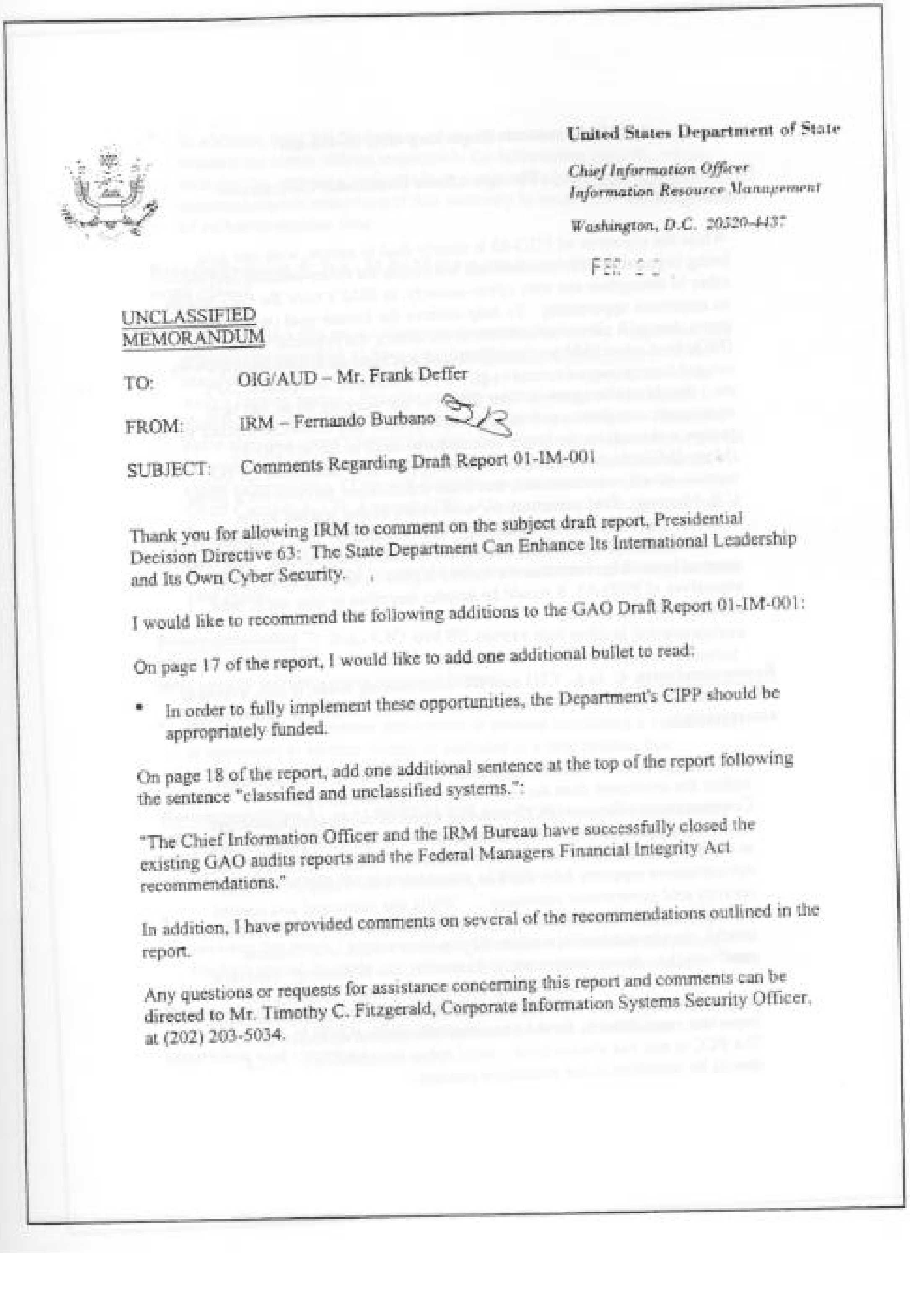
- On page 11 the draft alleges that PDD-63 requires a global approach "without regard to the level of our interdependencies." In fact, PDD-63 recognizes the first responsibility of the Federal Government is to perform essential national security missions and ensure the general public health and safety, and that this must involve a partnership with the private sector. By its very nature, analysis of the CIP international outreach priorities of the Federal Government requires assessment of interdependencies.

- On page 12, the draft contends the CICG is improperly engaging in "efforts to regulate the use of global information technology and systems." To the contrary, the international outreach plan speaks directly to the necessity of developing cooperative strategies not only between governments, but also between government, international organizations, and private industry. The strategy recognizes a balance must be drawn between



national security and law enforcement concerns and the protection of privacy and free markets. The plan also contains a section on agreed U.S. government policy to promote international research and development.

To conclude, the international plan is based on policies agreed to by the interagency group charged with implementing PDD-63. As the PDD-63 Foreign Affairs Functional Coordinator, I disagree with the draft report's contention that setting priorities for outreach to close allies and gearing our efforts to the development of the U.S. National Plan reflects a "constrained" approach or is inconsistent with PDD-63.



United States Department of State

Chief Information Officer
Information Resource Management

Washington, D.C. 20520-4437

FEB 2 [illegible]

UNCLASSIFIED
MEMORANDUM

TO: OIG/AUD – Mr. Frank Deffer

FROM: IRM – Fernando Burbano FB

SUBJECT: Comments Regarding Draft Report 01-IM-001

Thank you for allowing IRM to comment on the subject draft report, Presidential Decision Directive 63: The State Department Can Enhance Its International Leadership and Its Own Cyber Security.

I would like to recommend the following additions to the GAO Draft Report 01-IM-001:

On page 17 of the report, I would like to add one additional bullet to read:

- In order to fully implement these opportunities, the Department's CIPP should be appropriately funded.

On page 18 of the report, add one additional sentence at the top of the report following the sentence "classified and unclassified systems.":

"The Chief Information Officer and the IRM Bureau have successfully closed the existing GAO audits reports and the Federal Managers Financial Integrity Act recommendations."

In addition, I have provided comments on several of the recommendations outlined in the report.

Any questions or requests for assistance concerning this report and comments can be directed to Mr. Timothy C. Fitzgerald, Corporate Information Systems Security Officer, at (202) 203-5034.

APPENDIX G

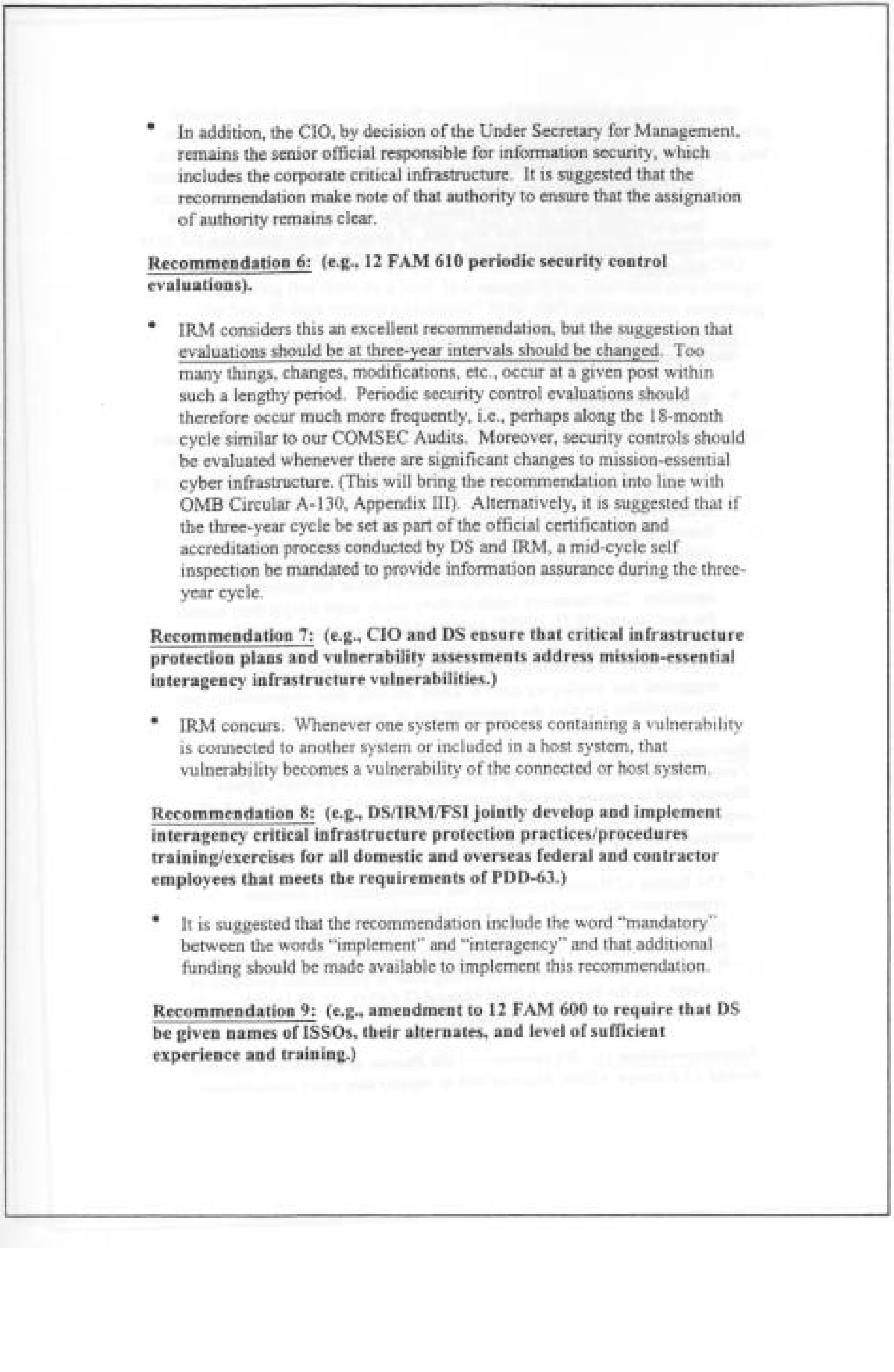
IRM Comments Regarding OIG 01-IM-001

__Recommendation 1:__ (e.g., Foreign Affairs Functional Coordinator responsibilities).

- While the objective of PDD-63 is clearly dual in nature, with one goal being to provide U.S. international leadership for cyber-security and the other to strengthen our own cyber-security, in IRM's view the OIG misses an important opportunity. To help achieve the former goal (we already know they will play a critical role in the latter), the potential role of our IMOs (and other IRM personnel) abroad and their daily relationships with several foreign organizations (e.g., PTTs, Telephone companies, ISPs, etc.) should not be ignored. Our IMOs, at the working level, can help encourage, coordinate, and support such official and unofficial entities to review and consider the larger international need to fulfill PDD-63. (Many IMOs do this already in reviewing potential candidates for ISP service, new line connections, and other information services for a given U.S. Mission). IRM personnel are well aware of and trained in the concepts and need for "sustainability" and "reliability" (key components of CIP and cyber infrastructure) of systems and communications. This is an internal knowledge base that we should exploit in helping achieve the objectives of PDD-63. It would be helpful therefore to also enlist their assistance in this matter.

__Recommendation 4:__ (e.g., CIO and DS determining what, if any, overseas minimum essential cyber infrastructure should be subject to vulnerability assessments).

- This is a good, sound recommendation. But neither here nor anywhere within the document does the reader see our operational Post Communication Centers (PCC) as being a part of the larger Department cyber-security infrastructure. Yet on page one of the draft paper (footnote to the Executive Summary), it clearly states that *"mission-essential cyber infrastructure supports core mission processes, which support national security and government continuity"*. While our command and control systems may now be sufficiently well protected and defended from cyber-attacks, the physical infrastructure they operate within is of dubious condition (i.e., doors, alarms, etc.). Moreover, the technology used now inside the PCC will ultimately migrate to newer, more "Internet-like" programs in the future where cyber-security (for data) will become an important consideration for the classified information operation as well. The PCC is and has always been critical cyber infrastructure. PCCs should be consulted in the evaluation process.



- In addition, the CIO, by decision of the Under Secretary for Management, remains the senior official responsible for information security, which includes the corporate critical infrastructure. It is suggested that the recommendation make note of that authority to ensure that the assignation of authority remains clear.

Recommendation 6: (e.g., 12 FAM 610 periodic security control evaluations).

- IRM considers this an excellent recommendation, but the suggestion that evaluations should be at three-year intervals should be changed. Too many things, changes, modifications, etc., occur at a given post within such a lengthy period. Periodic security control evaluations should therefore occur much more frequently, i.e., perhaps along the 18-month cycle similar to our COMSEC Audits. Moreover, security controls should be evaluated whenever there are significant changes to mission-essential cyber infrastructure. (This will bring the recommendation into line with OMB Circular A-130, Appendix III). Alternatively, it is suggested that if the three-year cycle be set as part of the official certification and accreditation process conducted by DS and IRM, a mid-cycle self inspection be mandated to provide information assurance during the three-year cycle.

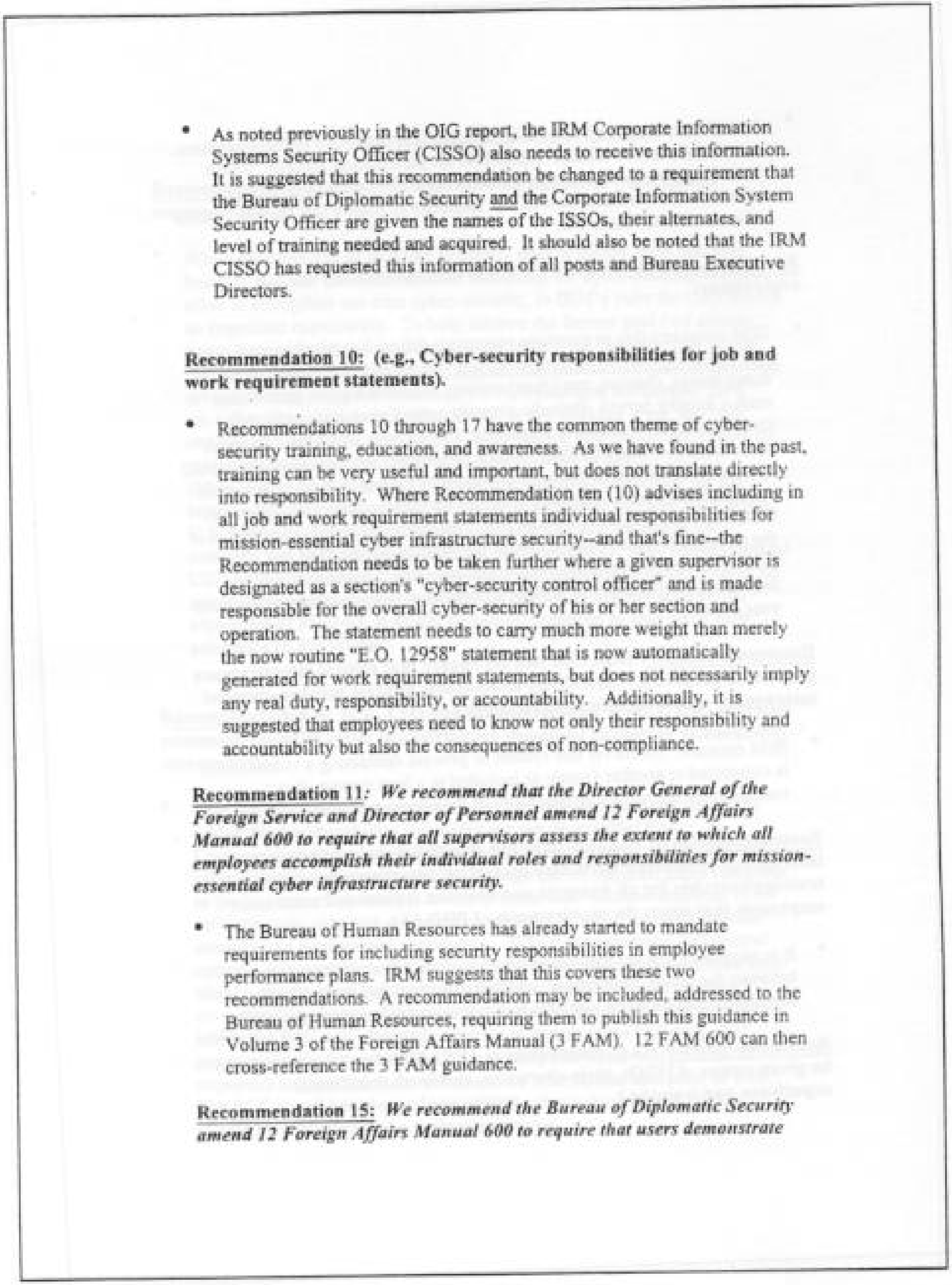
Recommendation 7: (e.g., CIO and DS ensure that critical infrastructure protection plans and vulnerability assessments address mission-essential interagency infrastructure vulnerabilities.)

- IRM concurs. Whenever one system or process containing a vulnerability is connected to another system or included in a host system, that vulnerability becomes a vulnerability of the connected or host system.

Recommendation 8: (e.g., DS/IRM/FSI jointly develop and implement interagency critical infrastructure protection practices/procedures training/exercises for all domestic and overseas federal and contractor employees that meets the requirements of PDD-63.)

- It is suggested that the recommendation include the word "mandatory" between the words "implement" and "interagency" and that additional funding should be made available to implement this recommendation.

Recommendation 9: (e.g., amendment to 12 FAM 600 to require that DS be given names of ISSOs, their alternates, and level of sufficient experience and training.)



- As noted previously in the OIG report, the IRM Corporate Information Systems Security Officer (CISSO) also needs to receive this information. It is suggested that this recommendation be changed to a requirement that the Bureau of Diplomatic Security and the Corporate Information System Security Officer are given the names of the ISSOs, their alternates, and level of training needed and acquired. It should also be noted that the IRM CISSO has requested this information of all posts and Bureau Executive Directors.

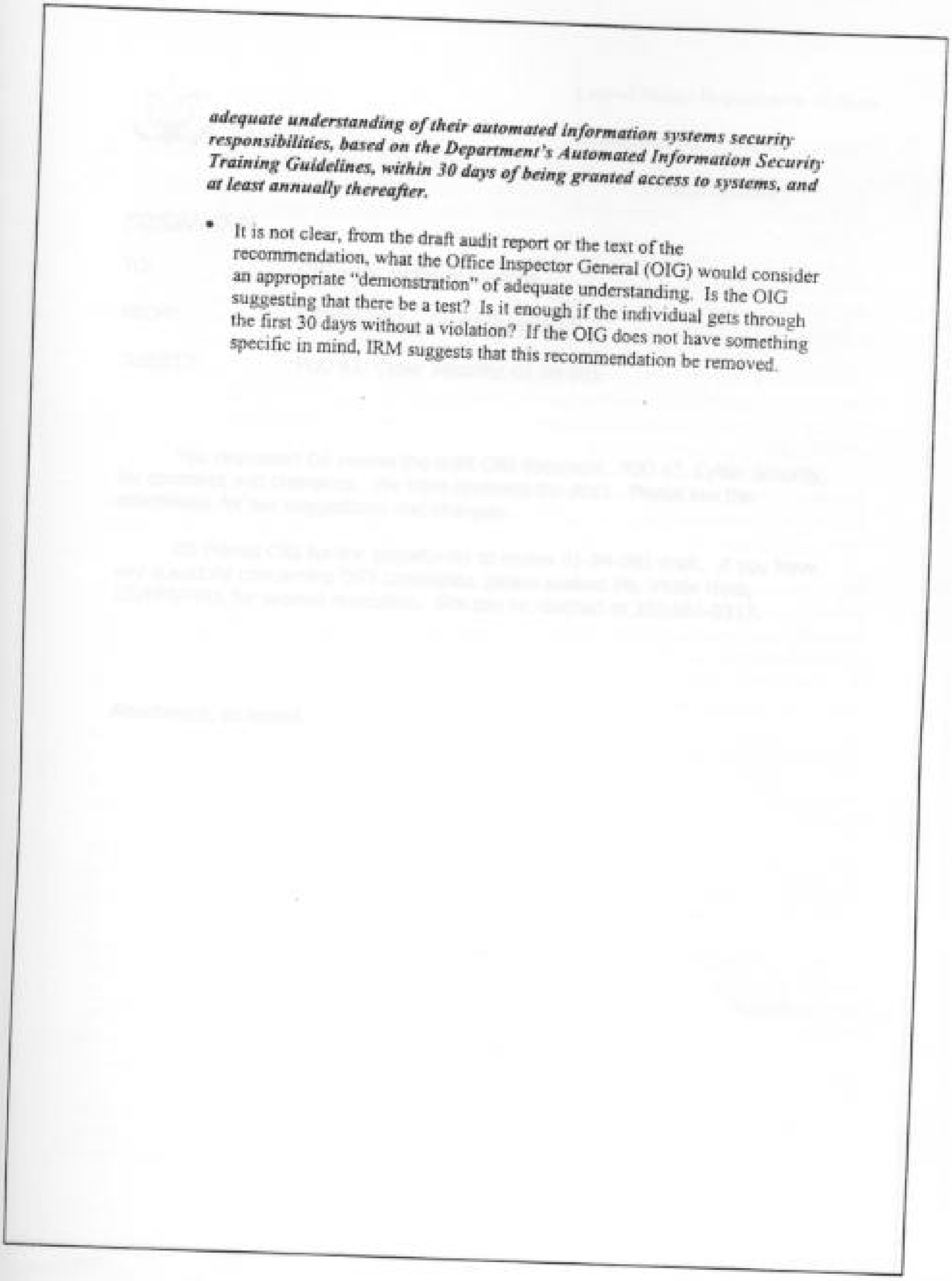
Recommendation 10: (e.g., Cyber-security responsibilities for job and work requirement statements).

- Recommendations 10 through 17 have the common theme of cyber-security training, education, and awareness. As we have found in the past, training can be very useful and important, but does not translate directly into responsibility. Where Recommendation ten (10) advises including in all job and work requirement statements individual responsibilities for mission-essential cyber infrastructure security--and that's fine--the Recommendation needs to be taken further where a given supervisor is designated as a section's "cyber-security control officer" and is made responsible for the overall cyber-security of his or her section and operation. The statement needs to carry much more weight than merely the now routine "E.O. 12958" statement that is now automatically generated for work requirement statements, but does not necessarily imply any real duty, responsibility, or accountability. Additionally, it is suggested that employees need to know not only their responsibility and accountability but also the consequences of non-compliance.

Recommendation 11: ***We recommend that the Director General of the Foreign Service and Director of Personnel amend 12 Foreign Affairs Manual 600 to require that all supervisors assess the extent to which all employees accomplish their individual roles and responsibilities for mission-essential cyber infrastructure security.***

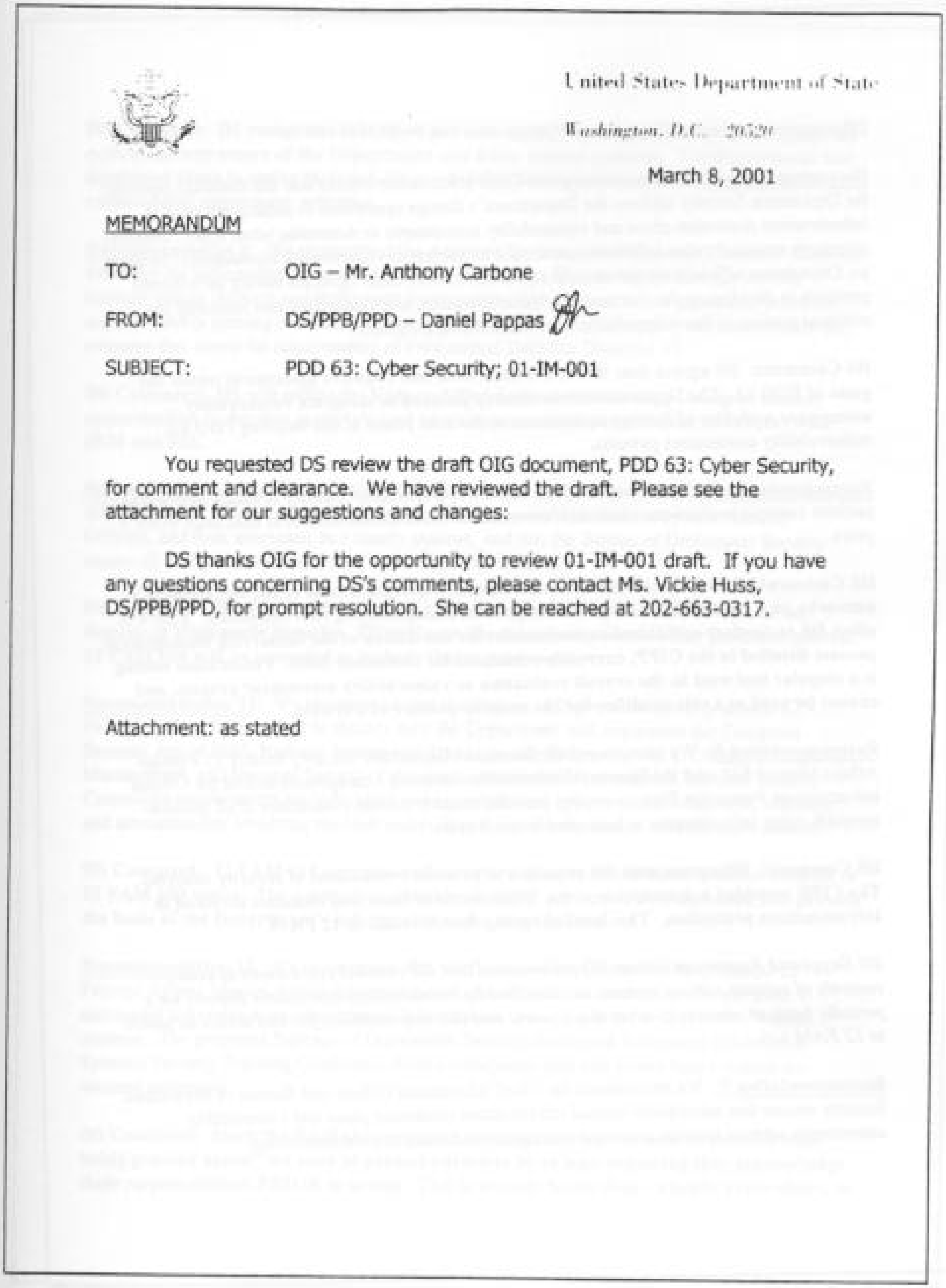
- The Bureau of Human Resources has already started to mandate requirements for including security responsibilities in employee performance plans. IRM suggests that this covers these two recommendations. A recommendation may be included, addressed to the Bureau of Human Resources, requiring them to publish this guidance in Volume 3 of the Foreign Affairs Manual (3 FAM). 12 FAM 600 can then cross-reference the 3 FAM guidance.

Recommendation 15: ***We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users demonstrate***



adequate understanding of their automated information systems security responsibilities, based on the Department's Automated Information Security Training Guidelines, within 30 days of being granted access to systems, and at least annually thereafter.

- It is not clear, from the draft audit report or the text of the recommendation, what the Office Inspector General (OIG) would consider an appropriate "demonstration" of adequate understanding. Is the OIG suggesting that there be a test? Is it enough if the individual gets through the first 30 days without a violation? If the OIG does not have something specific in mind, IRM suggests that this recommendation be removed.



United States Department of State

Washington, D.C. 20520

March 8, 2001

MEMORANDUM

TO: OIG – Mr. Anthony Carbone

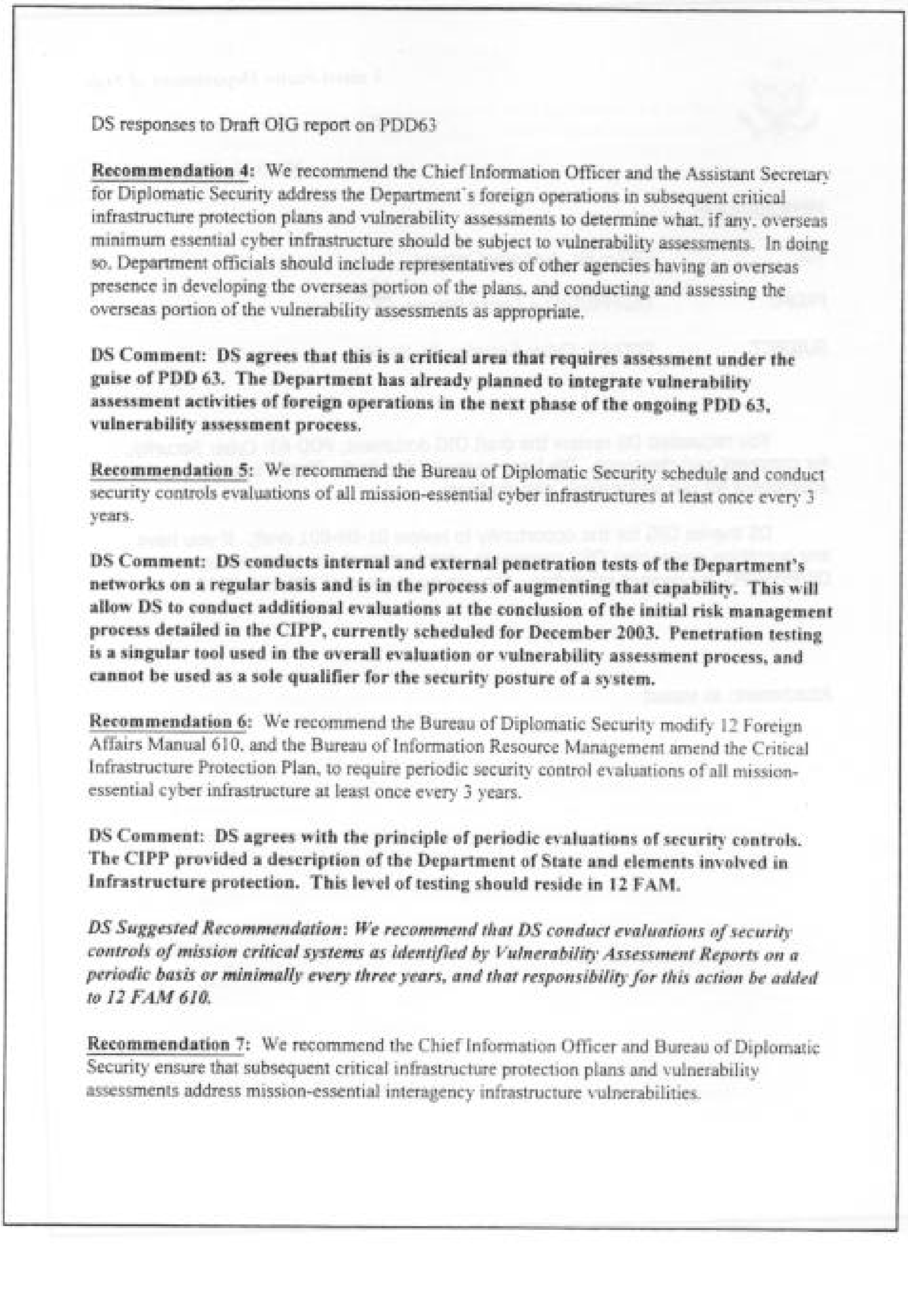
FROM: DS/PPB/PPD – Daniel Pappas

SUBJECT: PDD 63: Cyber Security; 01-IM-001

You requested DS review the draft OIG document, PDD 63: Cyber Security, for comment and clearance. We have reviewed the draft. Please see the attachment for our suggestions and changes:

DS thanks OIG for the opportunity to review 01-IM-001 draft. If you have any questions concerning DS's comments, please contact Ms. Vickie Huss, DS/PPB/PPD, for prompt resolution. She can be reached at 202-663-0317.

Attachment: as stated



DS responses to Draft OIG report on PDD63

Recommendation 4: We recommend the Chief Information Officer and the Assistant Secretary for Diplomatic Security address the Department's foreign operations in subsequent critical infrastructure protection plans and vulnerability assessments to determine what, if any, overseas minimum essential cyber infrastructure should be subject to vulnerability assessments. In doing so, Department officials should include representatives of other agencies having an overseas presence in developing the overseas portion of the plans, and conducting and assessing the overseas portion of the vulnerability assessments as appropriate.

DS Comment: DS agrees that this is a critical area that requires assessment under the guise of PDD 63. The Department has already planned to integrate vulnerability assessment activities of foreign operations in the next phase of the ongoing PDD 63, vulnerability assessment process.

Recommendation 5: We recommend the Bureau of Diplomatic Security schedule and conduct security controls evaluations of all mission-essential cyber infrastructures at least once every 3 years.

DS Comment: DS conducts internal and external penetration tests of the Department's networks on a regular basis and is in the process of augmenting that capability. This will allow DS to conduct additional evaluations at the conclusion of the initial risk management process detailed in the CIPP, currently scheduled for December 2003. Penetration testing is a singular tool used in the overall evaluation or vulnerability assessment process, and cannot be used as a sole qualifier for the security posture of a system.

Recommendation 6: We recommend the Bureau of Diplomatic Security modify 12 Foreign Affairs Manual 610, and the Bureau of Information Resource Management amend the Critical Infrastructure Protection Plan, to require periodic security control evaluations of all mission-essential cyber infrastructure at least once every 3 years.

DS Comment: DS agrees with the principle of periodic evaluations of security controls. The CIPP provided a description of the Department of State and elements involved in Infrastructure protection. This level of testing should reside in 12 FAM.

DS Suggested Recommendation: We recommend that DS conduct evaluations of security controls of mission critical systems as identified by Vulnerability Assessment Reports on a periodic basis or minimally every three years, and that responsibility for this action be added to 12 FAM 610.

Recommendation 7: We recommend the Chief Information Officer and Bureau of Diplomatic Security ensure that subsequent critical infrastructure protection plans and vulnerability assessments address mission-essential interagency infrastructure vulnerabilities.

DS Comment: DS recognizes that there are interagency interdependencies that impact the critical infrastructure of the Department and other federal agencies. The Department has developed plans to assess these interdependencies during subsequent phases of PDD 63 vulnerability assessment activities.

Recommendation 8: We recommend the Assistant Secretary for Diplomatic Security, Assistant Secretary for Information Resource Management, and the Director of the Foreign Service Institute jointly develop and implement interagency critical infrastructure protection practices and procedures training and exercises for all federal and contractor employees domestically and overseas that meets the requirements of Presidential Decision Directive 63.

DS Comment: DS will utilize the Vulnerability Assessment Working Group to identify opportunities to develop materials and courses to meet this requirement in concert with IRM and FSI.

Recommendation 9: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that it be given the names of Information System Security Officers, and their alternates, in a timely manner, and that the Bureau of Diplomatic Security ensure all designees have sufficient experience and training.

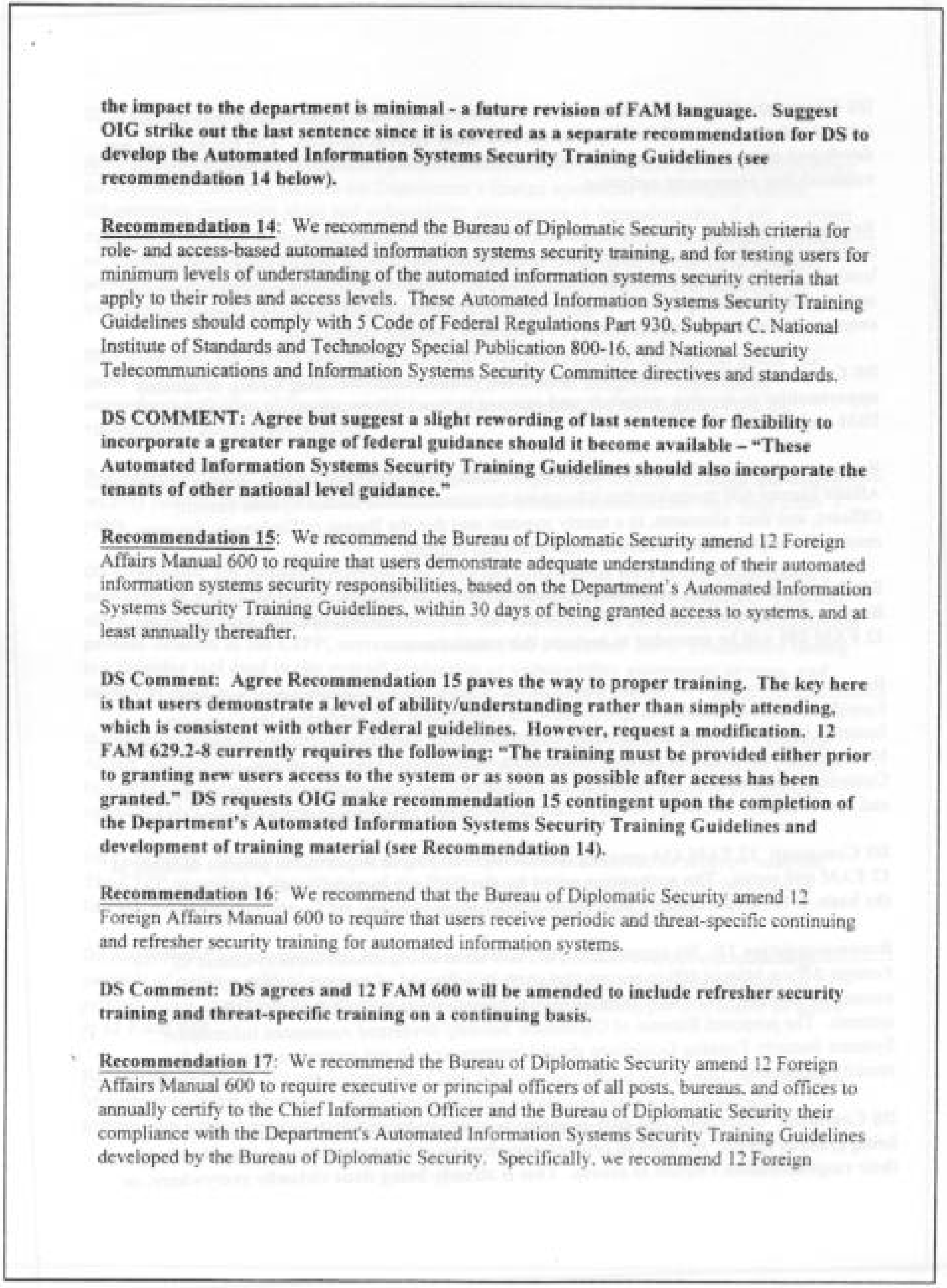
DS Comment: Written notification of appointments or changes should be sent to the Bureau of Diplomatic Security. DS will provide the information to other pertinent offices. 12 FAM 600 will be amended to include this requirement.

Recommendation 12: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to specify how the Department will implement the Computer Security Act of 1987, National Institute of Standards and Technology, U.S. Office of Personnel Management, and National Security Telecommunications and Information Systems Security Committee requirements for individual and organizational cyber security awareness, training, and accountability involving mission-essential automated information infrastructure security.

DS Comment: 12 FAM 614 contains authorities relating to Department policies detailed in 12 FAM 600 series. The authorities noted by the OIG are currently referenced and provide the basis of the Department's information technology policies.

Recommendation 13: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users be informed of, and acknowledge, their automated information security responsibilities prior to being granted access to Department systems. The proposed Bureaus of Diplomatic Security developed Automated Information Systems Security Training Guidelines should incorporate role and access based criteria for security awareness.

DS Comment: Since the FAM only requires security training "as soon as possible after being granted access" we need to protect ourselves by at least requiring they acknowledge their responsibilities PRIOR to access. This is already being done virtually everywhere, so



the impact to the department is minimal - a future revision of FAM language. Suggest OIG strike out the last sentence since it is covered as a separate recommendation for DS to develop the Automated Information Systems Security Training Guidelines (see recommendation 14 below).

__Recommendation 14__: We recommend the Bureau of Diplomatic Security publish criteria for role- and access-based automated information systems security training, and for testing users for minimum levels of understanding of the automated information systems security criteria that apply to their roles and access levels. These Automated Information Systems Security Training Guidelines should comply with 5 Code of Federal Regulations Part 930, Subpart C, National Institute of Standards and Technology Special Publication 800-16, and National Security Telecommunications and Information Systems Security Committee directives and standards.

DS COMMENT: Agree but suggest a slight rewording of last sentence for flexibility to incorporate a greater range of federal guidance should it become available – "These Automated Information Systems Security Training Guidelines should also incorporate the tenants of other national level guidance."

__Recommendation 15__: We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users demonstrate adequate understanding of their automated information systems security responsibilities, based on the Department's Automated Information Systems Security Training Guidelines, within 30 days of being granted access to systems, and at least annually thereafter.

DS Comment: Agree Recommendation 15 paves the way to proper training. The key here is that users demonstrate a level of ability/understanding rather than simply attending, which is consistent with other Federal guidelines. However, request a modification. 12 FAM 629.2-8 currently requires the following: "The training must be provided either prior to granting new users access to the system or as soon as possible after access has been granted." DS requests OIG make recommendation 15 contingent upon the completion of the Department's Automated Information Systems Security Training Guidelines and development of training material (see Recommendation 14).

__Recommendation 16__: We recommend that the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require that users receive periodic and threat-specific continuing and refresher security training for automated information systems.

DS Comment: DS agrees and 12 FAM 600 will be amended to include refresher security training and threat-specific training on a continuing basis.

__Recommendation 17__: We recommend the Bureau of Diplomatic Security amend 12 Foreign Affairs Manual 600 to require executive or principal officers of all posts, bureaus, and offices to annually certify to the Chief Information Officer and the Bureau of Diplomatic Security their compliance with the Department's Automated Information Systems Security Training Guidelines developed by the Bureau of Diplomatic Security. Specifically, we recommend 12 Foreign

Affairs Manual 600 require that principal officers certify their organizations have documented that everyone who has access to the Department's systems has been given compliant site-specific security awareness training relevant to their roles and responsibilities in accordance with the Department's Automated Information Systems Security Training Guidelines

DS Comment: Certification can be a means of ensuring that documentation of user briefings is accurately maintained at post. Compliance can be measured through DS security assessments conducted by Regional Computer Security Officers (RCSO), DS/IST/ACD and OIG. This can also provide a means for posts to identify training deficiencies to assist the DS in prioritizing training resources.

DS Suggested Recommendation: We recommend 12 Foreign Affairs Manual 600 require the executive or principle officer of all posts and bureaus to annually certify to DS and CIO, compliance with the Department of State AIS Security Training Guidelines developed by Diplomatic Security.

Prepared by:
DS/IST/ACD, comments were incorporated from DSTC where applicable.